EXHIBIT B

Excerpts of SW-SEC00388332, formatted for legibility

DOCUMENT PRODUCED IN NATIVE FORMAT

DOCUMENT PRODUCED IN NATIVE FORMAT

	A	C	D	E	F	H	I	J	K	M
1										
2	#	System	Process	Control Number	Control Language	Issue Short Name	Description of Control Deviation Identified by IA	Exception Type (MW, SD, CD)	Remediated Y/N	Why the impact is not pervasive?
9	7	Backup	User Access Management	2.1	The Company maintains password requirements for all financially significant systems and databases, including the requirements that they be changed periodically, meet minimum length requirements, retain password history, and require password complexity, as allowed by the application, system, or database. Web hosted applications may not require active directory authentication. If access is limited by a password and requires log in into Active Directory (includes system accounts) the requirements for password change, password complexity and password history are not considered necessary.	Password requirements not met (Access)	Backup appears to utilize TUL / AD first and foremost. However, application guidance notes that, in instances where TUL / AD is not a possibility, the application-specific password policy is used. Per inspection of the Backup policy, only a portion of the password requirements are met – (1) complexity is enabled and (2) minimum characters are defined. However, (3) a maximum password age is not configured as required, nor is (4) a password history requirement.	CD	N	The primary access path for Backup is through TUL / AD. Instances in which users are logging in outside of TUL / AD is not nearly as common and thus plays a role in limiting the risk found in the exception. Additionally, the application-specific password configuration detail meets some of the requirements, but not all, meaning there is security in the application-specific password detail just not to the extent that the control language requires. Lastly, the quarterly user access review performed over Backup provides comfort over restricted access.
10	8	Backup	Access Provisioning	2.2	New users are provisioned access in accordance with the SolarWinds System Groups Matrix. Any additional access required, including access to super user or admin responsibilities, require approval from manager, IT and/or the system owner. Additional NetSuite access to sensitive worldwide financial results requires approval by the Financial Controller or the VP of WW Finance.	Lack of access approval prior to provisioning (Access)	1 user (Denis Savitsky) of 8 samples that was not approved for new access	CD	Y	Despite the lack of support evidencing proper access approval prior to provisioning, any form of inappropriate access would ultimately be identified through the quarterly user access reviews performed by management per system.
11	9	Backup	User Access Management	2.5	User access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory users) and databases.	Lack of independent reviewer (Access)	Holtzman Partners noted the review was performed by Igor Lushchik, Manager Operations Engineering. As Igor has privileged / write access to numerous layers within the system, it would be expected that a secondary reviewer without privileged access would also perform a review. As such, this is considered an exception.	CD	Y	The quarterly review acts as a catch all related to controls 2.2, 2.3, and 2.4; however, if those controls are performed correctly (access provisioning, access termination, and transfer access removal), this limits the potential for widespread issues resulting from the missed review of a specific database. As it relates to this specific exception, control 2.2 (access provisioning) would theoretically act as a mitigating control as a way to ensure proper access changes are granted appropriately. Assuming that control is functioning as expected, the risk of a privileged user performing a quarterly review without a secondary approver would be reduced.
13	11	N-Activate	Access Provisioning	2.2	New users are provisioned access in accordance with the SolarWinds System Groups Matrix. Any additional access required, including access to super user or admin responsibilities, require approval from manager, IT and/or the system owner. Additional NetSuite access to sensitive worldwide financial results requires approval by the Financial Controller or the VP of WW Finance.	Lack of access approval prior to provisioning (Access)	2 users (Zakariya Weatherstone and Xiaobing Liu) of 30 samples did not have sufficient evidence of approval for their access prior to provisioning.	CD	Y	Despite the lack of support evidencing proper access approval prior to provisioning, any form of inappropriate access would ultimately be identified through the quarterly user access reviews performed per system.
14	12	N-Activate	User Access Management	2.5	User access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory users) and databases.	Lack of independent reviewer (Access)	Holtzman Partners noted the review was performed by Tim Drury, Manager Systems Engineering. As Tim has privileged / write access to numerous layers within the system, it would be expected that a secondary reviewer without privileged access would also perform a review. As such, this is considered an exception.	CD	N	The quarterly review acts as a catch all related to controls 2.2, 2.3, and 2.4; however, if those controls are performed correctly (access provisioning, access termination, and transfer access removal), this limits the potential for widespread issues resulting from a privileged user performing a review without secondary review of his/her access. As it relates to this specific exception, control 2.2 (access provisioning) would theoretically act as a mitigating control as a way to ensure proper access changes are granted appropriately. Assuming that control is functioning as expected, the risk of a privileged user performing a quarterly review without a secondary approver would be reduced.
17	15	Netsuite	Access Review	2.5	User access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory users) and databases.	Insufficient evidence of control performance, i.e. completeness, timeliness (Access)	Terminated users who appeared with active Netsuite access were not captured and requested for removal during the Q4 Netsuite user access review.	CD	N	In an effort to address the potential pervasiveness of the deficiency noted, SolarWinds management performed a full review over terminations for the 2019 year specific to NetSuite in order to ensure the issue was not pervasive beyond what was noted in the exception language. Additionally, for the terminated employees noted within the exception language, despite the delay in access removal, management noted no user logins took place after the stated termination dates of each employee tested.
18	16	Netsuite / Zuora UK / Zuora Canada	Terminations	2.3	When an employee is terminated, access to Active Directory and financial systems is removed in a timely manner, as follows: - within 24 hours for administrator access - within 7 days for all other levels of access	Access removal not timely (Access)	3 terminated users (of 25 samples) retained active access in Netsuite. While AD access was tested and found to be deactivated appropriately, noted that users in Netsuite and Zuora UK/Canada systems can access the application without utilizing SSO. Therefore, as communications of terminations were not communicated to the respective application teams following replacement of the HR system in October, noted that terminated users in Netsuite/Zuora retained active access past their termination dates.	CD	N	While it was noted the NetSuite termination timeliness deficiency extended into another deficiency within the NetSuite quarterly user access review, SolarWinds management performed a full review over terminations for the 2019 year specific to NetSuite in order to ensure the issue was not pervasive beyond what was noted in the exception language. Additionally, for the terminated employees noted within the exception language, despite the delay in access removal, management noted no user logins took place after the stated termination dates of each employee tested.
19	17	Orchestration / Updater / Connector	Access Review	2.5	User access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory users) and databases.	Insufficient evidence of control performance, i.e. completeness, timeliness (Access)	The Q2 2019 .Net License Orchestration review was performed by John Martinich, Senior Operations Manager, on 7/10/2019. However, it was noted that there was no evidence of John performing a full review. John's electronic signature was missing for review over the TDFSQL02 database. Additionally, screenshots in the Q1-Q3 reviews were not retained; therefore completeness of the review and timeliness of management follow-up items was not able to be determined. Lastly, secondary review over John's access was not performed.	CD	Y	While the exception was noted during the Q2 2019 review, the issue was remediated in 2019 during the quarterly reviews that followed. Additionally, there are mitigating controls that would theoretically work to address a missed quarterly review. The quarterly review acts as a catch all related to controls 2.2, 2.3, and 2.4; however, if those controls are performed correctly (access provisioning, access termination, and transfer access removal), this limits the potential for widespread issues resulting from the missed review of a specific database.
21	19	Policy	Access Policy	2	A user access management policy is established and documented for initiating, authorizing, recording, processing, reviewing a request for access rights, and evidence of retention. The user access management policy is reviewed and approved annually by the VP of IT. Evidence of review is documented and maintained.	Lack of evidence to show appropriate level of review/approval (Access)	Access policy was not reviewed during FY19.	CD	N	Despite the Access policy not being reviewed by management during the 2019 year, the controls detailed within the policy are active and in place among all employees relevant to the user access processes. A lack of management review of the policy document would not alter controls expected to be in place and functioning properly.
27	25	RMM	User Access Management	2.1	The Company maintains password requirements for all financially significant systems and databases, including the requirements that they be changed periodically, meet minimum length requirements, retain password history, and require password complexity, as allowed by the application, system, or database. Web hosted applications may not require active directory authentication. If access is limited by a password and requires log in into Active Directory (includes system accounts) the requirements for password change, password complexity and password history are not considered necessary.	Password requirements not met (Access)	RMM appears to utilize TUL / AD first and foremost. However, application guidance notes that, in instances where TUL / AD is not a possibility, the application-specific password policy is used. Per inspection of the RMM policy, only a portion of the password requirements are met – (1) complexity is enabled and (2) minimum characters are defined. However, (3) a maximum password age is not configured as required, nor is (4) a password history requirement.	CD	N	The primary access path for RMM is through TUL / AD. Instances in which users are logging in outside of TUL / AD is not nearly as common and thus plays a role in limiting the risk found in the exception. Additionally, the application-specific password configuration detail meets some of the requirements, but not all, meaning there is security in the application-specific password detail just not to the extent that the control language requires. Lastly, the quarterly user access review performed over RMM provides comfort over restricted access.
28	26	RMM	Access	2.2	New users are provisioned access in accordance with the SolarWinds System Groups Matrix.	Lack of access approval prior to	2 users (or 34 samples) did not have evidence of appropriate approval prior to	CD	Y	Despite the lack of support evidencing proper access approval prior to provisioning, any form of inappropriate access would ultimately be identified through the quarterly user access

	A	C	D	E	F	H	I	J	K	M
29	27	RMM	Access Review	2.5	User access privileges are re-validated on a quarterly basis to confirm that users maintain appropriate access. These validation procedures are performed for all financially significant applications, systems (including Active Directory users) and databases.	Insufficient evidence of control performance, i.e. completeness, timeliness (Access)	Both the Q2 and Q3 reviews were not complete, as users were missed in the report generation due to a manual review report generation process. Additionally, management follow-up items in the Q3 review were not completed until PwC request on 11/18; therefore follow-ups were not actioned timely following review.	CD	N	Despite the deficiencies noted in the RMM access reviews for Q2 and Q3 2019, there are mitigating controls that would theoretically work to address a missed quarterly review. The quarterly review acts as a catch all related to controls 2.2, 2.3, and 2.4; however, if those controls are performed correctly (access provisioning, access termination, and transfer access removal), this limits the potential for widespread issues resulting from the missed review of a specific database.
30	28	Data Foundry	Access	N/a	Control 6.16 Password requirements have also been established for Data Foundry servers	Insufficient evidence of control	Exception Noted: For 2 servers (both running the Solaris OS) of 4 servers tested,	CD	Y	Although password complexity was not set, other components of a secure password were configured, lowering the risk of inappropriate access to the servers.